AIOTI

ALLIANCE FOR INTERNET OF THINGS INNOVATION

AIOTI position on the EU Cybersecurity Act Proposal

16 May 2018

AIOTI WG04 – IoT Policy

AIOTI
ALLIANCE FOR INTERNET OF THINGS INNOVATION

EU Cybersecurity Act Proposal

In order to scale up the EU's response to cyber-attacks, improve cyber resilience and increase trust in the Digital single market, the European Commission has proposed a Regulation on the European Union Cybersecurity Agency - ENISA - and on the establishment of an EU cybersecurity certification framework.

Need for trust

The digital transformation of the economy and society is providing new solutions and services but also a vast diversity of new cyber threats: linked to monetization methods, attacks on democracies, denials of services, as well as personal data theft. There is an emergency to react and restore trust in a connected world, by implementing for instance security-by-design approaches or baseline security and privacy requirements for achieving confidentiality, integrity and authenticity security objectives. And wherever necessary, these requirements should be established for the complete supply chain of IoT products and services.

AIOTI members welcome the Cybersecurity Act that aims at creating a European cybersecurity certification market and agree that cybersecurity certification plays a critical role in increasing trust and security that are crucial for the Digital Single Market.

AIOTI members call on European decision-makers to keep the framework voluntary in general, with the market and customers deciding in which cases a voluntary and/or mandatory certification is needed (for instance, mandatory certification could be envisaged for critical infrastructure and for critical IoT solutions).

Reference to standards

European and international standards from IEC, ISO, CEN/CENELEC, ETSI are at the core of the activities of the industry and widely used for certification. For competitiveness purposes, certification schemes shall be based on international and European standards to provide common rules, increase transparency, and allow a fair comparison of products and suppliers.

Sector-specific requirements

Cybersecurity has a broad applicability, in different sectors and markets, with different constraints and in practice there is no "one-size-fits-all" solution. Each European certification scheme to be adopted must be tailored and consider specificities, constraints and risks linked to the products and services to be covered.

The same shall apply in terms of the standards against which certification will be made against: standard levels applicable to all sectors shall be encouraged as a common baseline and complemented by sector specific standards level according to targeted products/services/sectors. The challenge is that the cybersecurity act needs to be applicable by all players, while providing enough guarantee that it will not be misused and, finally, reinforce security instead of reducing it.

Importance of security 'processes'

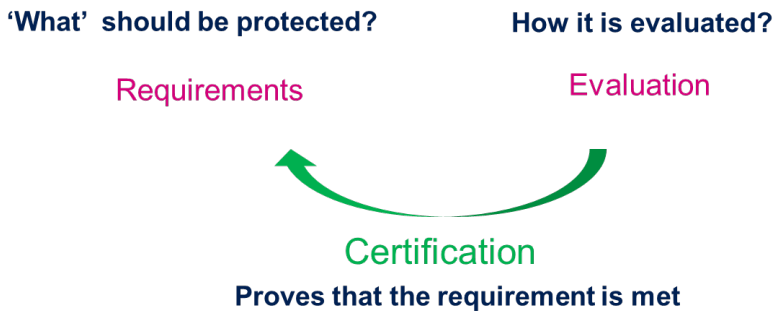
The current proposal only refers to certification of ICT products and services. AIOTI members agree that security of processes should also be included in the text. It is also of utmost importance to consider the products, processes and services throughout their life-cycle.

Scalable framework

Due to the very different nature of applications, assets and threats, all stakeholders are committed to provide the best cost/benefit ratio of their security solutions and welcome the scalability of the certification framework. As the current scope of the Regulation is very broad and covers all "ICT products and services", it is therefore important to adopt a scalable approach, according to the risks and criticality of products and services to be covered by EU schemes.

This scalable framework should be based on a risk-based approach: the provider shall perform risk assessment on the entire solution, identify critical security functions answering to the questions 'what has to be protected', and, assuming residual risks and related impact, 'which threats should be considered ', 'what is the level of robustness expected'. Companies should establish risk-based rules that ensure adequate and continuous protection across all IoT layers, with appropriate security measures depending on the risk assessment.

Semiconductor components manufacturers have products differentiated by their robustness to attacks. Attack potential can be low (well-knows attacks, performed through the network, with low cost equipment and generic knowledge), moderate (more sophisticated attacks, with physical access to the devices, low cost hacking tools, basic hacking skills) or high (all known 'state-of-the-art' attacks scenario, high cost equipment's and high skilled hackers) . In the specific case of semiconductor components, security evaluations of components by third party accredited laboratories with appropriate 'ethical hacking skills' provide trust in the effectiveness of the security features vs the attack potential.



Security assurance levels

AIOTI members have different positions on security assurance levels proposed in the Cybersecurity Act:

- Some members welcome these levels as it provides a degree of confidence in the claim or asserted security qualities of a process, a product or service. For basic level, security assessment verifying compliance to claimed security properties can be done by 'checklists'. While for substantial and high, security assessment verifying robustness versus a given attack potential (time, cost, skills, etc.) shall be performed by accredited assessment laboratories with appropriate and comparable 'ethical hacking' capabilities
- For others, three security levels which are proposed in the European Commission could be further expanded to alleviate fear of security as a barrier for small and medium sized enterprises.
- Some members also suggest to move the definition of assurance levels to each specific certification scheme. Each scheme might have different assurance levels depending on its goals, sector, stakeholders etc., which would be a more efficient way than an ex ante definition/"one fits for all".

All members agree that industry involvement is needed to detail the requirements for each level.

Self-assessment

Self-assessment is a well-established and, at the same time, rigorous process in Europe for assessing compliance with requirements. Self-assessment is a core principle of the New Legislative Framework for gaining market access in regulated areas and operating under the Presumption of Conformity as laid down in Regulation 765/2008. Self-assessment therefore should be allowed in the context of this cybersecurity framework but should not be mixed up with an assessment by an independent certification accredited body.

Self-assessment shall be based on compliance with security rules and guidelines, providing transparency and allowing fair comparison of different providers.

Third party assessment

For third party assessment, certification scheme constrained in time and cost should be developed in a cost-efficient way to stay attractive without compromising the aimed security levels.

For areas where risk assessment justifies high risk, e.g. in the context of critical infrastructures as defined in the NIS Directive as well as other critical IoT solutions, accredited third-party certification is required for mutual recognition.

For highest security levels, semiconductor manufacturers are requested to deliver products resisting to the most sophisticated attacks, assessed by state-of-the-art laboratories. A currently well-established and standardized scheme is Common Criteria (CC, ISO/IEC 15408) already implemented in many EU Member States and other countries with mutual recognition agreement (SOG-IS MRA). Recognition by all Member Stated is needed to prevent EU market fragmentation. If Common Criteria certification is reference certification scheme for security products such as firewall or secure chips, it is not relevant for other types of products such as industrial products, which have their own certification schemes/standards.

Multi-stakeholder participation

Cybersecurity can only be addressed in an appropriate way in a public-private ecosystem where also society and relevant stakeholders are involved, share knowledge and become more aware. Therefore, any policy-making efforts concerning any certification should strike a fair balance between legitimate interests of all stakeholders, including the society, consumers, industries, and policy-makers.

Industry, for example, already performs certification in specific domains and it is essential to preserve the value of already existing certificates and establish a migration path to the new framework.

To prevent duplication of certification for the public and private sectors and ensure schemes are fit for purpose, industry should have an active role in their elaboration: it shall be allowed to request for the preparation of the scheme and be involved in the various stages of the process (i.e. the scoping, the preparation, the adoption and the maintenance of EU certification schemes). Overall, the role of the industry including the SMES, especially, during the preparation of a European candidate certification schemes, should be clarified in order to ascertain that all interests are represented.

Industry already performs certification in specific domains and it is essential to preserve the value of already existing certificates and establish a migration path to the new framework.

Validity of the certificate

The EU certification framework needs to be agile and flexible to adapt to a wide scope of ICT products and services. For this reason, the validity of the certificate should be defined in each scheme, on a case-by-case basis.

In addition, it should be considered whether it is appropriate that the renewal/update of cybersecurity certificates (Art. 48) and accreditation of cybersecurity bodies (Art. 51) may be provided under the same conditions. This consideration should be made mainly due to the evolving nature of cybersecurity domain and the likelihood of different security requirements over various years. Therefore, it is recommended that renewals/updates are granted based on compliance with current standards/requirements/best practices.

Transparency and openness of certification information

Transparency and openness to the information package regarding certification is necessary, including information such as a clear overlook on the EU harmonization aspects and which standards are referred in the schemes.

